

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 1 1 日
Date of Application:

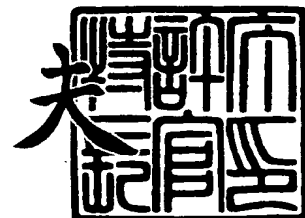
出 願 番 号 特 願 2 0 0 2 - 2 9 9 6 5 8
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 2 9 9 6 5 8]

出 願 人 株 式 会 社 リ コ ー
Applicant(s):

2 0 0 3 年 8 月 2 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0207088

【提出日】 平成14年10月11日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00 530

【発明の名称】 アクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体

【請求項の数】 19

【発明者】

 【住所又は居所】 東京都大田区中馬込1丁目3番6号
 株式会社リコー内

 【氏名】 金井 洋一

【特許出願人】

 【識別番号】 000006747

 【氏名又は名称】 株式会社リコー

 【代表者】 桜井 正光

【代理人】

 【識別番号】 100084250

 【弁理士】

 【氏名又は名称】 丸山 隆夫

 【電話番号】 03-3590-8902

【手数料の表示】

 【予納台帳番号】 007250

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【包括委任状番号】 0207936

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 アクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体

【特許請求の範囲】

【請求項 1】 所定のネットワークに接続されたアクセス制御サーバであって、

前記ネットワークを介して電子データの作成者の端末から前記電子データを受信する電子データ受信手段と、

前記受信された電子データのデータ種別を示す情報および前記受信された電子データに係るユーザのユーザ ID を含むワークフロー情報を受信するワークフロー情報受信手段と、

電子データに対するユーザの種別ごとのアクセス権限を示すアクセス権限テンプレートを電子データのデータ種別ごとに 1 つ以上格納するテンプレート格納手段と、

前記格納された 1 つ以上のアクセス権限テンプレートから、前記受信されたワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出手段と、

前記抽出されたアクセス権限テンプレートに、各ユーザの前記ユーザ ID を挿入して、前記受信された電子データに対する前記各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成手段と、

を有することを特徴とするアクセス制御サーバ。

【請求項 2】 前記受信された電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信手段と、

前記アクセス制限情報に基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成手段と、

前記生成されたアクセス制限データを前記ネットワークを介して送信するデータ送信手段と、

を有することを特徴とする請求項 1 記載のアクセス制御サーバ。

【請求項 3】 前記テンプレート格納手段は、

前記ユーザの種別として、前記電子データの作成者、前記電子データの承認者、および前記アクセス制限データの送信先のユーザが設定されている前記アクセス権限テンプレートを格納することを特徴とする請求項 2 記載のアクセス制御サーバ。

【請求項 4】 前記アクセス制限データ生成手段は、

予め自サーバに格納されたセキュリティポリシーに基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする請求項 2 または 3 記載のアクセス制御サーバ。

【請求項 5】 前記アクセス制限データ生成手段は、

前記受信された電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする請求項 2 から 4 のいずれか 1 項に記載のアクセス制御サーバ。

【請求項 6】 所定のネットワークに接続され、電子データに対するアクセス制御を行うアクセス制御サーバを用いた電子データ発行ワークフロー処理方法であって、

前記アクセス制御サーバが、前記ネットワークを介して電子データの作成者の端末から前記電子データを受信する電子データ受信工程と、

前記アクセス制御サーバが、前記受信した電子データのデータ種別を示す情報および前記受信された電子データに係るユーザのユーザ ID を含むワークフロー情報を受信するワークフロー情報受信工程と、

前記アクセス制御サーバが、電子データに対するユーザの種別ごとのアクセス権限を示すアクセス権限テンプレートを電子データのデータ種別ごとに 1 つ以上格納するテンプレート格納工程と、

前記アクセス制御サーバが、前記格納した 1 つ以上のアクセス権限テンプレートから、前記受信したワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出工程と、

前記アクセス制御サーバが、前記抽出したアクセス権限テンプレートに、各ユーザの前記ユーザ ID を挿入して、前記受信した電子データに対する前記各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成工程

と、

を有することを特徴とする電子データ発行ワークフロー処理方法。

【請求項 7】 前記アクセス制御サーバが、前記受信した電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信工程と、

前記承認情報受信後に、前記アクセス制御サーバが、前記アクセス制限情報に基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成工程と、

前記アクセス制御サーバが、前記生成されたアクセス制限データを前記ネットワークを介して送信するデータ送信工程と、

を有することを特徴とする請求項 6 記載の電子データ発行ワークフロー処理方法。

【請求項 8】 前記アクセス制御サーバが、前記アクセス制限情報に基づいて、前記受信した電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成工程と、

前記アクセス制御サーバが、前記受信した電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信工程と、

前記アクセス制御サーバが、前記承認情報を受信すると、前記生成されたアクセス制限データを前記ネットワークを介して送信するデータ送信工程と、

を有することを特徴とする請求項 6 記載の電子データ発行ワークフロー処理方法。

【請求項 9】 前記テンプレート格納処理は、

前記ユーザの種別として、前記電子データの作成者、前記電子データの承認者、および前記アクセス制限データの送信先のユーザが設定されている前記アクセス権限テンプレートを格納することを特徴とする請求項 7 または 8 記載の電子データ発行ワークフロー処理方法。

【請求項 10】 前記アクセス制限データ生成工程は、

前記アクセス制御サーバが、予め自サーバに格納したセキュリティポリシーに基づいて、前記受信した電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする請求項 7 から 9 のいずれか 1 項に記載の電子データ発行ワークフロー処理方法。

タ発行ワークフロー処理方法。

【請求項 1 1】 前記アクセス制限データ生成工程は、

前記受信した電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする請求項 7 から 1 0 のいずれか 1 項に記載の電子データ発行ワークフロー処理方法。

【請求項 1 2】 電子データの作成者により作成された前記電子データの受信制御を行う電子データ受信処理と、

前記受信された電子データのデータ種別を示す情報および前記受信された電子データに係るユーザのユーザ I D を含むワークフロー情報の受信制御を行うワークフロー情報受信処理と、

電子データに対するユーザの種別ごとのアクセス権限を示す 1 つ以上のアクセス権限テンプレートを電子データのデータ種別ごとに格納するテンプレート格納処理と、

前記格納された 1 つ以上のアクセス権限テンプレートから、前記受信されたワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出処理と、

前記抽出されたアクセス権限テンプレートに、各ユーザの前記ユーザ I D を挿入して、前記受信された電子データに対する前記各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成処理と、

をコンピュータに実行させるためのプログラム。

【請求項 1 3】 前記受信された電子データの発行が承認者により承認された旨の承認情報の受信制御を行う承認情報受信処理と、

前記承認情報受信後に、前記アクセス制限情報に基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成処理と、

前記生成されたアクセス制限データの送信制御を行うデータ送信処理と、

をコンピュータに実行させるための請求項 1 2 記載のプログラム。

【請求項 1 4】 前記アクセス制限情報に基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限デー

タ生成処理と、

前記受信された電子データの発行が承認者により承認された旨の承認情報の受信制御を行う承認情報受信処理と、

前記承認情報の受信を認識すると、前記生成されたアクセス制限データの送信制御を行うデータ送信処理と、

をコンピュータに実行させるための請求項 12 記載のプログラム。

【請求項 15】 前記テンプレート格納処理は、

前記ユーザの種別として、前記電子データの作成者、前記電子データの承認者、および前記アクセス制限データの送信先のユーザが設定されている前記アクセス権限テンプレートを格納することを特徴とする請求項 13 または 14 記載のプログラム。

【請求項 16】 前記アクセス制限データ生成処理は、

セキュリティポリシーに基づいて、前記受信された電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする請求項 13 から 15 のいずれか 1 項に記載のプログラム。

【請求項 17】 前記アクセス制限データ生成処理は、

前記受信された電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする請求項 13 から 16 のいずれか 1 項に記載のプログラム。

【請求項 18】 請求項 12 から 17 のいずれか 1 項に記載のプログラムを実行するコンピュータ装置。

【請求項 19】 請求項 12 から 17 のいずれか 1 項に記載のプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、アクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体に関し、特に、ファイルの作成者により指定されたファイルの種類、ファイルの承認者および配布先などに基づ

いて、作成したファイルに対するアクセス権限の制御を行うアクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体に関する。

【0 0 0 2】

【従来の技術】

従来、ネットワーク上の電子データに対する各ユーザの利用権限が記録されたアクセスコントロールリスト（Access Control List：ACL）に基づいて、発行したファイルのアクセス制御を行っていた。ACLを用いて電子データに対するアクセス制御を行う従来技術として、特開 2 0 0 1 - 1 4 2 8 7 4 号公報（以下、特許文献 1）が開示するところの文書管理システム、および特開 2 0 0 1 - 1 9 5 2 9 5 号公報（以下、特許文献 2）が開示するところの統合型技術文書管理装置があった。

【0 0 0 3】

特許文献 1 および引用文献 2 では、文書を作成して登録し、承認されると文書を印刷可能な P D F（登録商標）ファイルと印刷不可能な P D F ファイルに変換し、利用権限に応じて、閲覧できるファイルを制限していた。

【0 0 0 4】

【特許文献 1】

特開 2 0 0 1 - 1 4 2 8 7 4 号公報

【特許文献 2】

特開 2 0 0 1 - 1 9 5 2 9 5 号公報

【0 0 0 5】

【発明が解決しようとする課題】

しかしながら、従来の技術では、電子データによるファイルを作成する度に、ユーザごとにファイルの利用権限を示す情報を入力する必要があり、多数のユーザがそのファイルを利用する場合、利用権限を示すデータを生成するために多大な労力および時間を費やさなければならなかった。

【0 0 0 6】

本発明は、上記問題点に鑑みてなされたものであり、電子データに対する利用

権限を示すデータ（ACL）を容易に生成し、その生成した利用権限を示すデータに基づいて電子データに対するアクセス制御を行うアクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体を提供することを目的とする。

【0007】

【課題を解決するための手段】

かかる目的を達成するため、請求項1記載の発明は、所定のネットワークに接続されたアクセス制御サーバであって、ネットワークを介して電子データの作成者の端末から電子データを受信する電子データ受信手段と、受信された電子データのデータ種別を示す情報および受信された電子データに係るユーザのユーザIDを含むワークフロー情報を受信するワークフロー情報受信手段と、電子データに対するユーザの種別ごとのアクセス権限を示すアクセス権限テンプレートを電子データのデータ種別ごとに1つ以上格納するテンプレート格納手段と、格納された1つ以上のアクセス権限テンプレートから、受信されたワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出手段と、抽出されたアクセス権限テンプレートに、各ユーザのユーザIDを挿入して、受信された電子データに対する各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成手段と、を有することを特徴とする。

【0008】

また、請求項2記載の発明によれば、請求項1記載のアクセス制御サーバにおいて、受信された電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信手段と、アクセス制限情報に基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成手段と、生成されたアクセス制限データをネットワークを介して送信するデータ送信手段と、を有することを特徴とする。

【0009】

また、請求項3記載の発明によれば、請求項2記載のアクセス制御サーバにおいて、テンプレート格納手段は、ユーザの種別として、電子データの作成者、電

子データの承認者、およびアクセス制限データの送信先のユーザが設定されているアクセス権限テンプレートを格納することの特徴とする。

【0010】

また、請求項4記載の発明によれば、請求項2または3記載のアクセス制御サーバにおいて、アクセス制限データ生成手段は、予め自サーバに格納されたセキュリティポリシーに基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成することの特徴とする。

【0011】

また、請求項5記載の発明によれば、請求項2から4のいずれか1項に記載のアクセス制御サーバにおいて、アクセス制限データ生成手段は、受信された電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することの特徴とする。

【0012】

また、請求項6記載の発明は、所定のネットワークに接続され、電子データに対するアクセス制御を行うアクセス制御サーバを用いた電子データ発行ワークフロー処理方法であって、アクセス制御サーバが、ネットワークを介して電子データの作成者の端末から電子データを受信する電子データ受信工程と、アクセス制御サーバが、受信した電子データのデータ種別を示す情報および受信された電子データに係るユーザのユーザIDを含むワークフロー情報を受信するワークフロー情報受信工程と、アクセス制御サーバが、電子データに対するユーザの種別ごとのアクセス権限を示すアクセス権限テンプレートを電子データのデータ種別ごとに1つ以上格納するテンプレート格納工程と、アクセス制御サーバが、格納した1つ以上のアクセス権限テンプレートから、受信したワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出工程と、アクセス制御サーバが、抽出したアクセス権限テンプレートに、各ユーザのユーザIDを挿入して、受信した電子データに対する各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成工程と、を有することの特徴とする。

【0013】

また、請求項 7 記載の発明によれば、請求項 6 記載の電子データ発行ワークフロー処理方法において、アクセス制御サーバが、受信した電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信工程と、承認情報受信後に、アクセス制御サーバが、アクセス制限情報に基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成工程と、アクセス制御サーバが、生成されたアクセス制限データをネットワークを介して送信するデータ送信工程と、を有することを特徴とする。

【0 0 1 4】

また、請求項 8 記載の発明によれば、請求項 6 記載の電子データ発行ワークフロー処理方法において、アクセス制御サーバが、アクセス制限情報に基づいて、受信した電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成工程と、アクセス制御サーバが、受信した電子データの発行が承認者により承認された旨の承認情報を受信する承認情報受信工程と、アクセス制御サーバが、承認情報を受信すると、生成されたアクセス制限データをネットワークを介して送信するデータ送信工程とを有することを特徴とする。

【0 0 1 5】

また、請求項 9 記載の発明によれば、請求項 7 または 8 記載の電子データ発行ワークフロー処理方法において、テンプレート格納処理は、ユーザの種別として、電子データの作成者、電子データの承認者、およびアクセス制限データの送信先のユーザが設定されているアクセス権限テンプレートを格納することを特徴とする。

【0 0 1 6】

また、請求項 1 0 記載の発明によれば、請求項 7 から 9 のいずれか 1 項に記載の電子データ発行ワークフロー処理方法において、アクセス制限データ生成工程は、アクセス制御サーバが、予め自サーバに格納したセキュリティポリシーに基づいて、受信した電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする。

【0 0 1 7】

また、請求項 1 1 記載の発明によれば、請求項 7 から 1 0 のいずれか 1 項に記

載の電子データ発行ワークフロー処理方法において、アクセス制限データ生成工程は、受信した電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする。

【0018】

また、請求項12記載の発明は、電子データの作成者により作成された電子データの受信制御を行う電子データ受信処理と、受信された電子データのデータ種別を示す情報および受信された電子データに係るユーザのユーザIDを含むワークフロー情報の受信制御を行うワークフロー情報受信処理と、電子データに対するユーザの種別ごとのアクセス権限を示す1つ以上のアクセス権限テンプレートを電子データのデータ種別ごとに格納するテンプレート格納処理と、格納された1つ以上のアクセス権限テンプレートから、受信されたワークフロー情報に含まれる電子データのデータ種別情報に対応したアクセス権限テンプレートを抽出するテンプレート抽出処理と、抽出されたアクセス権限テンプレートに、各ユーザのユーザIDを挿入して、受信された電子データに対する各ユーザのアクセス権限を示すアクセス権限情報を生成するアクセス権限情報生成処理と、をコンピュータに実行させることを特徴とする。

【0019】

また、請求項13記載の発明によれば、請求項12記載のプログラムにおいて、受信された電子データの発行が承認者により承認された旨の承認情報の受信制御を行う承認情報受信処理と、承認情報受信後に、アクセス制限情報に基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成処理と、生成されたアクセス制限データの送信制御を行うデータ送信処理と、をコンピュータに実行させることを特徴とする。

【0020】

また、請求項14記載の発明によれば、請求項12記載のプログラムにおいて、アクセス制限情報に基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成するアクセス制限データ生成処理と、受信された電子データの発行が承認者により承認された旨の承認情報の受信制御を行う承認情報受信処理と、承認情報の受信を認識すると、生成されたアクセス制限データの

送信制御を行うデータ送信処理と、をコンピュータに実行させることを特徴とする。

【0021】

また、請求項15記載の発明によれば、請求項13または14記載のプログラムにおいて、テンプレート格納処理は、ユーザの種別として、電子データの作成者、電子データの承認者、およびアクセス制限データの送信先のユーザが設定されているアクセス権限テンプレートを格納することを特徴とする。

【0022】

また、請求項16記載の発明によれば、請求項13から15のいずれか1項に記載のプログラムにおいて、アクセス制限データ生成処理は、セキュリティポリシーに基づいて、受信された電子データにアクセス制限をかけて、アクセス制限データを生成することを特徴とする。

【0023】

また、請求項17記載の発明によれば、請求項13から16のいずれか1項に記載のプログラムにおいて、アクセス制限データ生成処理は、受信された電子データにアクセス制限をかけ、かつデータフォーマットの変換を行い、アクセス制限データを生成することを特徴とする。

【0024】

また、請求項18記載の発明によれば、請求項12から17のいずれか1項に記載のプログラムを実行することを特徴とする。

【0025】

また、請求項19記載の発明によれば、請求項12から17のいずれか1項に記載のプログラムを記録したことを特徴とする。

【0026】

【発明の実施の形態】

（第1の実施形態）

本実施形態において、文書発行ワークフローシステムは、発行したドキュメントを審査・承認した後、保護ドキュメントを発行する。なお、本明細書において、「ドキュメント」とは、単なる文書を示すものに限定されず、電子データによ

るものであれば、プログラム、画像、データベースまたは他のものであってもよい。

【0027】

図1は、本発明の第1の実施形態における文書発行ワークフローシステムを示す第1の図である。以下、図1を用いて、本実施形態における文書発行ワークフローシステムの構成について説明する。

【0028】

文書発行ワークフローシステムは、作成者端末1と、アクセス制御サーバ2と、承認者端末3と、ユーザ端末4と、を有する。また、アクセス制御サーバ2は、作成者端末1、承認者端末3、およびユーザ端末4とそれぞれネットワークを介して接続されている。

【0029】

作成者端末1は、ドキュメント作成者により操作される情報処理装置であり、例えばパーソナルコンピュータであってもよい。作成者端末1は、表示装置（例えば、LCD（Liquid Crystal Display））と、入力装置（例えば、キーボード）と、記録装置（例えば、FDD（Floppy（登録商標） Disk Drive）、HDD（Hard Disk Drive））とを有する。

【0030】

また、作成者端末1は、自身に格納された作成クライアントプログラム10を実装する。例えば、作成クライアントプログラム10は、Webブラウザで実現するようにしてもよいし、他にもIBM社のグループウェア製品であるLotus Notes（登録商標）のクライアント用プログラムであってもよい。

【0031】

作成者端末1は、電子データであるドキュメント11と、ドキュメント11の属性等を示すワークフロー情報12とを生成し、アクセス制御サーバ2に送信する。

【0032】

アクセス制御サーバ2は、ドキュメント11およびACLなどを管理する情報

処理装置であって、例えばWebサーバであってもよい。アクセス制御サーバ2は、ワークフロープログラム20およびドキュメント保護プログラム21により動作する。

【0033】

また、アクセス制御サーバ2は、例えばHDDなどの記録装置22を有する。記録装置22は、ACLテンプレートDB（ACLテンプレートデータベース）23と、ACLDDB（ACLデータベース）24と、ワークフローオブジェクト25とを格納する。

【0034】

ACLテンプレートDB23は、ドキュメント11の種類（ファイルタイプ）に応じた1つ以上のACLテンプレートを管理するデータベースである。ACLテンプレートとは、ドキュメント11へのアクセス権限が示されているACL生成時に用いられるACLのテンプレート情報である。

【0035】

ACLDDB24は、ワークフロープログラム20が生成したACLを管理するデータベースである。

【0036】

ワークフローオブジェクト25は、ドキュメント11とワークフロー情報12aとをそれぞれ対応付けて組み合わせた情報である。

【0037】

承認者端末3は、ドキュメント配布の承認（approve）または却下（reject）を判断する承認者により操作される情報処理装置であって、例えばパーソナルコンピュータであってもよい。承認者端末3は、表示装置（例えば、LCD）と、入力装置（例えば、キーボード）と、記録装置（例えば、FDD、HDD）とを有する。

【0038】

また、承認者端末3は、承認者クライアントプログラム30を格納し、承認者クライアントプログラム30は、承認者端末3に各動作を実行させる。

【0039】

ユーザ端末 4 は、ドキュメント 1 1（保護ドキュメント 1 3）を利用するユーザにより操作される情報処理装置であって、例えばパーソナルコンピュータであってもよい。また、ユーザ端末 4 は、表示装置（例えば、LCD）と、入力装置（例えば、キーボード）と、記録装置（例えば、FDD、HDD）とを有する。

【0040】

以下、図 1 を用いて、本実施形態における文書発行ワークフローシステムによる動作について説明する。

【0041】

まず、作成者端末 1 は、ドキュメント作成者が承認依頼を希望するドキュメント 1 1 と、ドキュメント 1 1 に係る情報が示されるワークフロー情報 1 2 とを取得する。なお、ドキュメント 1 1 およびワークフロー情報 1 2 は、必ずしも作成者端末 1 が生成したものでなくてもよく、作成者端末 1 が、接続されている所定のネットワークを介して受信したものであってもよい。また、ドキュメント 1 1 およびワークフロー情報 1 2 が所定の携帯可能な記録媒体に記録されており、作成者端末 1 が、その記録媒体を読み取って取得してもよい。

【0042】

図 2 は、本発明の第 1 の実施形態における作成者端末 1 のワークフロー情報 1 2 作成時の画面表示を示す図である。作成者クライアントプログラム 1 0 は、図 2 に示されるような画面を作成者端末 1 に設けられた表示装置の画面上に表示させる。

【0043】

図 2 に示されているように、ワークフロー情報 1 2 の生成画面には、ドキュメント 1 1 の「ファイルタイトル」、「ファイルタイプ」、「作成者」、「ファイル内容」、「配布先」、および「承認者」の入力欄が設けられており、ドキュメント作成者は、作成者端末 1 に設けられている入力装置を介して、上記の各入力欄に情報を入力する。作成者クライアントプログラム 1 0 は、各入力欄に入力された情報に基づいて、ワークフロー情報 1 2 を生成する。

【0044】

「ファイルタイトル」は、ドキュメント 1 1 のタイトル（表題）を示す。また

、「ファイルタイプ」は、作成者端末 1 内に予め 1 つ以上定義および設定されており、作成者端末 1 は、例えばプルダウンメニューにより 1 種類以上のファイルタイプから所定のものを選択するようにしてもよい。「ファイル内容」には、承認を依頼するドキュメント 11 のファイル名が記載されており、その記載されたファイル名のドキュメント 11 がワークフロー情報 12 に添付される。

【0045】

「作成者」、「配布先」、および「承認者」の入力欄には、該当するユーザのユーザ ID を入力する。例えば、図 2 に示されているように、ユーザ ID として、各ユーザのメールアドレスを入力するようにしてもよい。なお、ユーザの種別は「作成者」、「配布先」、および「承認者」に限定されず、また各ユーザの数についても図 2 に示されるものに限定されない。

【0046】

図 3 は、本発明の第 1 の実施形態におけるワークフロー情報 12 の一例を示す図である。図 2 に示されるような入力情報に基づいて、図 3 に示されるようなワークフロー情報 12 が生成される。図 3 に示されているように、ワークフロー情報 12 には、ドキュメント 11 のファイルタイトル「Development of a new security system」と、ファイルタイプ「RESEARCH__PLAN」と、作成者「author__00@office.com」と、承認者「approver__01@office.com」と、ファイル内容（ドキュメントのファイル名）「theme__explanation.doc」と、配布先「user__10@office.com, user__11@office.com, user__20@office.com, user__21@office.com」といった情報が含まれている。

【0047】

なお、ワークフロー情報 12 の内容は、図 3 に示されるものに限定されず、他の内容の情報であってもよい。また、図 3 で、「ファイル内容」のところには承認を依頼するドキュメント 11 のファイル名が記載されているが、実際には、ドキュメント 11 のファイルそのものを示す。

【0048】

次に、作成者端末 1 は、ドキュメント 11 およびワークフロー情報 12 をアクセス制御サーバ 2 に送信し、ワークフローに流す。具体的には、作成者クライアントプログラム 10 は、図 2 のワークフロー情報 12 作成画面上に設けられている「承認（審査）依頼」ボタンのクリックを検出すると、ワークフロー情報 12 を生成し、生成したワークフロー情報 12 とともに対応するドキュメント 11 をアクセス制御サーバ 2 に送信するとしてもよい。

【0049】

アクセス制御サーバ 2 は、作成者端末 1 からドキュメント 11 およびワークフロー情報 12 を受信すると、ワークフロープログラム 20 は、受信したワークフロー情報 12 に対してユニーク（固有）なドキュメント ID（シリアル番号でも良い）を付与し、図 4 に示されるような例えば XML で記述したファイル（ワークフロー情報 12 a）を作成して、アクセス制御サーバ 2 内の記録装置（HDD）22 にドキュメント 11 とともに保存する。このとき、ドキュメント 11 とそれに対応するワークフロー情報 12 a とを関連付けた一組のデータをワークフローオブジェクト 25 とする。

【0050】

図 4 は、本発明の第 1 の実施形態における ID が付与されたワークフロー情報 12 a を示す図である。図 4 に示されているように、ワークフロー情報 12 a には、固有なドキュメント ID 「011237835」が付与されている。また、ワークフロー情報 12 a の現在の状態を示す「<status>」には、「wait_for_approval（承認待ち）」が示されており、図 4 に示されるワークフロー情報 12 a に対応するドキュメント 11 が承認者による審査（承認／却下）の結果を待っている状態であることが示されている。

【0051】

次に、ワークフロープログラム 20 は、ワークフロー情報 12 a に記載されている承認者端末 3（承認者のメールアドレス）に承認依頼の電子メールを送信する。承認依頼の電子メールには、ワークフロー情報 12 a に付与されたユニークなドキュメント ID を記載する。また、アクセス制御サーバ 2 を Web サーバとし、ワークフロープログラム 20 を Web サーバで稼動するプログラムとして実

現する場合、ワークフロープログラム 2 0 は、ワークフローオブジェクト 2 5 に該当する URL（例えば `http://server/workflow?wfid=011237835`）を電子メールに記載して承認者端末 3 に送信するようにしてもよい。

【0052】

図 5 は、本発明の第 1 の実施形態における文書発行ワークフローシステムを示す第 2 の図である。以下、図 5 を用いて、本実施形態における文書発行ワークフローシステムによる動作の説明を続ける。

【0053】

承認者端末 3 は、アクセス制御サーバ 2 から承認を依頼されているワークフローオブジェクト 2 5 が示されている電子メールを受信すると、承認者クライアントプログラム 3 0 を用いて、アクセス制御サーバ 2 に格納されているワークフローオブジェクト 2 5 の一覧を承認者端末 3 に設けられている表示装置の画面上に表示し、上記の電子メールにより承認を求められているワークフローオブジェクト 2 5 を選択する。

【0054】

承認者端末 3 は、承認者により例えば承認者端末 3 の入力装置に設けられている「承認ボタン」または「却下ボタン」が押下されたことを検出すると、必要に応じてワークフロー情報 1 2 a を改訂した上でワークフローオブジェクト 2 5 の「承認（A p p r o v e）」または「却下（R e j e c t）」を決定した旨の情報を認識する。

【0055】

承認者クライアントプログラム 3 0 は、ワークフローオブジェクト 2 5 に対して「承認」および「却下」のうちのどちらに決定されたかを判断し、「却下」されたことを認識すると（例えば却下ボタンが押されると）、却下されたこと（R e j e c t e d）を示す情報をアクセス制御サーバ 2 に送信する。アクセス制御サーバ 2 は、却下されたことを示す情報を受信すると、ワークフローオブジェクト 2 5 が却下されたことを示す情報を電子メールなどで作成者端末 1 に送信し、文書発行ワークフローシステムは、動作を終了する。

【0056】

承認者クライアントプログラム30は、ワークフローオブジェクト25が「承認」されたことを認識すると（例えば承認ボタンが押されると）、承認されたこと（Approval）を示す情報をアクセス制御サーバ2に送信する。

【0057】

ワークフロープログラム20は、アクセス制御サーバ2が承認された旨の情報を受信したことを認識すると、Approvalの対象となっているワークフローオブジェクト25についてワークフロー情報12aを改訂して、ワークフローの状態を示す項目（<status>）を「承認済み（Approved）」にする。

【0058】

次に、ワークフロープログラム20は、ワークフロー情報12aを「承認済み」にすると、その「承認済み」にしたワークフロー情報12aに基づいて、配布文書（ドキュメント11）のACLを生成する。そのACLの生成は例えば以下のようにして行う。なお、ワークフロー情報12aの内容は、図4に示されているものとする。

【0059】

図4に示されているワークフロー情報12aにおいて、承認されたドキュメント11のファイルタイプは、「RESEARCH__PLAN」であり、承認された後、<distributed_to>で列挙されている相手（配布先）のユーザ端末4に配布されることを表している。この例ではユーザIDとして電子メールアドレスを用いている。

【0060】

本実施形態では、アクセス制御サーバ2は、予め「RESEARCH__PLAN」、「CONTRACT」、「TOP__SECRET」などのファイルタイプごとにACLのテンプレートを格納しておく。なお、ここで挙げたファイルタイプはあくまでも一例であり、その名称および数などは他のものであってもよい。

【0061】

図6は、本発明の第1の実施形態におけるACLテンプレートを示す図である

。図6には、ファイルタイプが「RESEARCH_PLAN」であるドキュメントに対するACLテンプレートが示されている。

【0062】

図6に示されているように、ACLテンプレートには例えば「User type (ユーザタイプ)」、「Access type (アクセスタイプ)」、「Permission (許可情報)」、および「Requirements (処理要件)」といった項目がある。

【0063】

「ユーザタイプ」は、ドキュメントに対するアクセス権限を有するユーザの種類を示す項目であり、本実施形態では、「author (ドキュメント作成者)」、「Approver (承認者)」、「distribute_to (配布先のユーザ)」に区分されている。

【0064】

「アクセスタイプ」は、ドキュメントに対するアクセス方法の種類を示す項目であり、本実施形態では、「Read (ドキュメントの閲覧)」、「Write (ドキュメントの書き換え)」、「Print (ドキュメントの印刷)」、「Hardcopy (ドキュメントのハードコピー)」に区分されている。

【0065】

「許可情報」は、ドキュメント11のアクセスに対するAllowed (許可) / Denied (禁止) をユーザの種類 (User type) ごとに示すものである。例えば、図6に示されるACLテンプレートでは、「author (ドキュメント作成者)」は、「Read」、「Print」、および「Hardcopy」に関してアクセスが許可されており、「Write」に関してアクセスが禁止されている。

【0066】

「処理要件」は、ユーザ端末4が保護ドキュメント13を使用する際に、各アクセスタイプで要求される処理が示されている。例えば、図6のACLテンプレートでは、「処理要件」として、「PAC (Private Access)」、「BDP (Background Dot Pattern)」、「EBC (

Embedding Barcode)」、および「RAD (Record Audit Data)」が示されている。なお、「PAC」、「BDP」、「EBC」、および「RAD」については、後ほど詳述する。

【0067】

ワークフロープログラム20は、ワークフロー情報12aの「<status>」を「Approval (承認済み)」にした後、記録装置22内のACLテンプレートDB23で管理されている1つ以上のACLテンプレートから、ワークフロー情報12aに記述されているファイルタイプに対応したACLテンプレートを抽出する。本実施形態では、図5のように「ファイルタイプ」が「RESEARCH_PLAN」であるワークフロー情報12aに基づいて、ワークフロープログラム20は、図6に示されるような「RESEARCH_PLAN」のACLテンプレートを抽出する。

【0068】

次に、ワークフロープログラム20は、抽出したACLテンプレートに、ワークフロー情報12aに記述されている「作成者」、「承認者」、および「配布先」の情報(ユーザID)を挿入して、図7に示されるようなACLを生成する。

【0069】

図7は、本発明の第1の実施形態におけるACLの一例を示す図である。図7には、ワークフロー情報12aに示される「作成者」、「承認者」、および「配布先」(「author_00@office.com」、「approver_01@office.com」、「user_10@office.com」、「user_11@office.com」、「user_20@office.com」、「user_21@office.com」)それぞれにおけるアクセス権限が示されている。

【0070】

ワークフロープログラム20は、生成したACLを、生成時に用いたワークフロー情報12aに記述されていたドキュメントIDに関連付けてACLDB24に登録する。

【0071】

ワークフロープログラム 20 は、このようにして生成した ACL と、ドキュメント 11 とをドキュメント保護プログラム 21 に渡す。ドキュメント保護プログラム 21 は、生成された ACL に基づいて、ドキュメント 11 をプロテクトし、保護ドキュメント 13 を生成する。

【0072】

ワークフロープログラム 20 は、生成された保護ドキュメント 13 を取得し、取得した保護ドキュメント 13 を、配布先に指定されたユーザのユーザ端末 4 に電子メールなどで配布する。このとき、アクセス制御サーバ 2 は、保護ドキュメント 13 そのものをユーザ端末 4 に配布してもよい。

【0073】

ここで、図 5 を用いて、本実施形態における ACL を用いたドキュメント 11 に対するセキュリティ処理について説明する。なお、ユーザ端末 4 には、ドキュメントアクセスプログラムが実装されている。また、ユーザ端末 4 にはプリンタが接続されていることとする。

【0074】

ドキュメント保護プログラム 21 は、ドキュメント 11 にアクセス制御サーバ 2 の使用者（配布者）の入力操作に応じた処理要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEA など）を用いてドキュメント 11 を暗号化し、保護ドキュメント 13 を生成する処理を行う。

【0075】

ドキュメントアクセスプログラムは、ユーザ端末 4 の使用者（ユーザ）の入力操作に応じ、保護ドキュメント 13 を復号化するとともに設定されている処理要件に応じた印刷処理を自身で行うか、あるいはプリンタなどに実行させる処理を行うプログラムである。

【0076】

アクセス制御サーバ 2 は、ユーザがドキュメントを印刷しようとする場合に、ドキュメントアクセスプログラムからの要求に応じて ACL を参照し、ドキュメントにアクセスする権限があるか否か、処理要件がどのように設定されているかを取得するサーバである。

また、アクセス制御サーバ2は、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベースをさらに有するとする。

【0077】

ドキュメント保護プログラム21は、ドキュメント11およびACLを取得すると、復号に使用する暗号鍵（Key）を生成し、生成した暗号鍵を該当するドキュメントIDに関連づけて、記録装置22に登録する。

また、ドキュメント保護プログラム21は、暗号鍵を用いてドキュメント11を暗号化し、暗号化したドキュメント11に対してドキュメントIDを付加して保護ドキュメント13を生成する。

【0078】

アクセス制御サーバ2は、生成した保護ドキュメント13をネットワークを介して送信するなどしてユーザ端末4に渡す。

【0079】

ユーザが、ユーザ端末4の入力装置を介してドキュメントアクセスプログラムに対してドキュメントへのアクセスを指示すると、アクセスを要求されたドキュメントアクセスプログラムは、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメントアクセスプログラムは、ユーザ端末4の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。

【0080】

ドキュメントアクセスプログラムは、ユーザから入力されたユーザ名とパスワードとをアクセス制御サーバ2へ送信して、ユーザ認証を要求する。

【0081】

アクセス制御サーバ2は、ドキュメントアクセスプログラムから受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

ユーザを特定すると、アクセス制御サーバ2は、ACLDB24を参照し、ドキュメント11にアクセスする権限が配布先のユーザにあるか否かや、ユーザがドキュメント11にアクセスする際には、どのような処理要件が設定されているかを取得する。

ユーザにドキュメント 11 にアクセスする権限がある場合、アクセス制御サーバ 2 は、その旨を示す認証情報とともに、保護ドキュメント 13 を復号化するための暗号鍵とユーザがドキュメント 11 にアクセスする際の処理要件とをユーザ端末 4 を介してドキュメントアクセスプログラムに通知する。

【0082】

アクセス制御サーバ 2 から認証情報とともに、暗証鍵と処理要件とを取得したドキュメントアクセスプログラムは、暗号鍵を用いて保護ドキュメント 13 を復号化してドキュメント 11 に復元する。

ここで、ユーザがドキュメント 11 の印刷を要求している場合、ドキュメントアクセスプログラムは、処理要件を満たすようにプリンタに印刷処理を実行させる。例えば、保護ドキュメント 13 に BDP が処理要件として設定されている場合には、ドキュメント 11 の内容とともに地紋を印刷する。

【0083】

これにより、ドキュメント 11 を印刷する際に、配布者がユーザ各人に対して設定した処理要件を強制することが可能となる。

【0084】

また、アクセス制御サーバ 2 は、保護ドキュメント 13 をワークフローオブジェクト 25 の一部として記録装置 22 に保存しておき、その保護ドキュメント 13 にアクセスするための URL を電子メールでユーザ端末 4 に送るようにしてもよい（例えば `http://server/workflow?wfid=011237835` など）。

【0085】

また、アクセス制御サーバ 2 は、ユーザ端末 4 と同様に、作成者端末 1 および承認者端末 3 に対しても保護ドキュメント 13 または URL を送信するとしてもよい。

【0086】

上記のようにして、アクセス制御サーバ 2 は、承認されたドキュメントのアクセス権限を制限し、配布先のユーザにはアクセス制限のかかった保護ドキュメントを配布する。従って、アクセス制御サーバ 2 は、アクセス権限のあるユーザだ

けにドキュメントの内容の参照を許可し、また、印刷時においても権限を確認したうえでセキュリティ処理を施しながらアクセス権限を有するユーザに印刷させることができる。

【0087】

また、ドキュメント11が保護ドキュメント13を作成するのにふさわしくないデータフォーマットである場合、ワークフロープログラム20は、ドキュメント11から最適なデータフォーマットのドキュメントへの変換処理をあらかじめ施し、変換したドキュメントをドキュメント保護プログラム21に渡すようにするとよい。例えば、ドキュメント11がMicrosoft Word（登録商標）のファイルであって、ドキュメント保護プログラム21にとって最適なデータフォーマットがPDFファイルである場合、ワークフロープログラム20は、Microsoft Wordを起動して、WordファイルをAdobe Acrobat（登録商標）の機能を使ってPDFに変換した上で、ドキュメント保護プログラム21に渡す。従って、作成者端末1が作成するドキュメント11のデータフォーマットは、PDFに変換することができるものであれば何でも良いということになる。

【0088】

また、上記の実施形態では、アクセス制御サーバ2は、承認された後でドキュメント11から保護ドキュメント13を生成しているが、アクセス制御サーバ2がワークフロー情報12aを承認者端末3に「<status>」以外の部分を変更させない、つまり変更が必要な場合にはドキュメント11を却下するとしてもよい。その場合、アクセス制御サーバ2は、承認者端末3により審査（承認／却下）される前にあらかじめ保護ドキュメント13を生成しておき、生成した保護ドキュメント13をワークフローオブジェクト25の一部として保存しておくようにしてもよい。

【0089】

ここで、本実施形態における各印刷処理（「PAC」、「BDP」、「EBC」、「および「RAD」）について説明する。

【0090】

図 8 は、本発明の第 1 の実施形態におけるユーザ端末 4 0 2 による印刷動作を示す図である。図 8 に示されているように、ユーザ端末 4 0 2 は、ドキュメント印刷プログラム 4 2 1 と、プリンタドライバとを有する。また、ユーザ端末 4 0 2 は、プリンタ 4 0 3 と接続されている。

【 0 0 9 1 】

また、図 9 は、本発明の第 1 の実施形態におけるユーザ端末 4 0 2 に設けられている表示装置の画面上に表示されるプリントダイアログを示す図である。以下、図 8 および図 9 を用いて、印刷要件として P A C が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。

【 0 0 9 2 】

(1) ドキュメント印刷プログラム 4 2 1 は P A C が設定されているドキュメントを印刷する際には、図 9 に示すように、プリントダイアログを表示させた後に個人識別番号 (P e r s o n a l I d e n t i f i c a t i o n N u m b e r : P I N) を入力するダイアログをユーザ端末 4 0 2 の表示装置に表示させ、ユーザに P I N の入力を要求する。

(2) ユーザ端末 4 0 2 の入力装置を用いてユーザが P I N を入力すると、ドキュメント印刷プログラム 4 2 1 は、これをプリンタドライバに設定し、印刷を指示する。

プリンタドライバは、ドキュメントから P o s t s c r i p t などの P D L (P a g e D e s c r i p t i o n L a n g u a g e) で記述された印刷データ (P D L データ) を生成し、印刷部数や出力トレイなどの印刷ジョブ情報を記述した P J L (P r i n t J o b L a n g u a g e) データを P D L データの先頭に付加する。プリンタドライバはさらに P J L データの一部として P I N を付加し、その P J L データ付き P D L データをプリンタ 4 0 3 に送る。

プリンタ 4 0 3 は、P J L データ付き P D L データを受け取ると P J L データの内容を参照し、機密印刷用の P I N が含まれている場合は印刷出力せずにプリンタ 4 0 3 内部の記憶装置 (H D D など) に P J L データ付き P D L データを保存する。ユーザが P I N をプリンタ 4 0 3 のオペレーションパネルを介して入力すると、プリンタ 4 0 3 は入力された P I N を P J L データに含まれる P I N と

照合し、一致すれば P J L データに含まれていた印刷ジョブ条件（部数、トレイなど）を適用しながら P D L データに従って印刷出力する。

（3）プリンタドライバに P I N が設定できない、すなわち、プリンタ 4 0 3 が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。

【 0 0 9 3 】

このようにすることで、印刷実行後、プリンタ 4 0 3 のオペレーションパネルにおいて印刷実行前に入力したものと同一の P I N が入力されるまでドキュメントのプリントアウトがプリンタ 4 0 3 から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ 4 0 3 に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。

さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ 4 0 3 とやりとりを S S L（Secure Socket Layer）で保護してもよい。

【 0 0 9 4 】

また、ドキュメント印刷プログラム 4 2 1 を W i n d o w s（登録商標） D o m a i n のユーザ管理と連動させて、ユーザに対して P I N の入力を要求しないようにしてもよい。例えば、P I N をユーザに入力させるのではなく、W i n d o w s（登録商標） D o m a i n から現在ログオン中のユーザ I D を取得し、プリントデータとともにユーザ I D をプリンタ 4 0 3 へ送付するようにする。プリンタ 4 0 3 は、オペレーションパネルでユーザからのパスワード入力を受け、そのユーザ I D とパスワードとで W i n d o w s（登録商標） D o m a i n のユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。W i n d o w s（登録商標） D o m a i n に限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒な P I N 入力の手間を削減できる。

【 0 0 9 5 】

次に、印刷要件として E B C が設定されている場合のドキュメント印刷プロゲ

ラム 4 2 1 の動作について説明する。

(1) ドキュメント印刷プログラム 4 2 1 は、E B C が設定されているドキュメントを印刷する際にドキュメント I D を示すバーコード画像データ（又は、二次元コード）のデータを生成する。

(2) ドキュメント印刷プログラム 4 2 1 は、生成したバーコード画像データをスタンプ画像としてプリンタドライバにセットし、プリンタ 4 0 3 に印刷を指示する。

(3) プリンタドライバに E B C が設定できない、すなわち、プリンタ 4 0 3 がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0096】

このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキヤナのみがバーコードをデコードすることでドキュメント I D を取得し、そのドキュメント I D を基にハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキュリティ確保が可能となる。

【0097】

次に、印刷要件として B D P が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。

(1) ドキュメント印刷プログラム 4 2 1 は、B D P が設定されているドキュメントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する（例えば、I c h i r o , 2 0 0 2 / 0 8 / 0 4 2 3 : 4 7 : 1 0 ）。

(2) ドキュメント印刷プログラム 4 2 1 は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。

(3) ドキュメント印刷プログラム 4 2 1 は、生成した地紋画像をスタンプと

してプリンタドライバにセットし、プリンタ 403 にドキュメントの印刷を指示する。

(4) プリンタドライバに BDP が設定できない場合、すなわちプリンタ 403 が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0098】

このようにすることで、ドキュメントのプリントアウトの各ページには、印刷処理を実行したユーザ名と日時とが浮き出る地紋として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これは、EBC をサポートしていない複写機を使用する場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。

【0099】

また、「RAD」は、アクセス制御サーバ 2 内の保護ドキュメント 13 にアクセスしたユーザのログを記録する処理である。

【0100】

以上説明したように、本実施形態によれば、ドキュメント 11 に係るユーザ ID、およびファイルタイプなどが示されているワークフロー情報 12a と、ACL テンプレートと、を用いて ACL を生成する。従って、ドキュメント 11 に係るユーザ ID およびファイルタイプなどの簡単な情報を入力するだけで、ドキュメント 11 に対する複数のユーザの ACL を容易に生成することが可能となる。

【0101】

(第 2 の実施形態)

本発明の第 1 の実施形態では、ドキュメントのタイプ（ファイルタイプ）ごとに ACL テンプレートを設定しておく例を説明した。本実施形態では、所定のセキュリティポリシーに基づいて、保護ドキュメント 13 を保護する。

【0102】

図 10 に、アクセス制御サーバ 2 の記録装置 22 に登録されるセキュリティポリシーの一例を示す。

例えば、分野 (Category) が「技術文書 (Technical)」で機密レベル (Sensitivity) が「中 (Medium)」のドキュメント 11 は、カテゴリ (Category) が「技術 (Technical)」で階級 (Level) が「中 (Medium)」又は「上 (High)」のユーザに対して、閲覧 (Read) は許可するが RAD を要件とすること、印刷 (Print) を許可するが PAC と BDP と EBC と RAD とを要件とすること、及び、ハードコピー (Hardcopy) は許可しないことが規定されている。

アクセス制御サーバ 2 は、セキュリティポリシーのデータをどのような形で記録保持していても構わない。なお、XML を用いて記述してもよい。

【0103】

図 11 は、本発明の第 2 の実施形態におけるドキュメント 11 のファイルタイプとセキュリティポリシーとの対応を示すマッピングテーブルを示す図である。図 11 のようなマッピングテーブルは、アクセス制御サーバ 2 内の記録装置 22 に格納されている。

【0104】

図 11 に示されているように、マッピングテーブルでは、ドキュメントのファイルタイプと、Security attributes (セキュリティ属性) とが関連付けられている。セキュリティ属性には、「Category (分野)」および「Sensitivity (機密レベル)」が含まれる。

【0105】

以下、図 5 を用いて、セキュリティポリシーをそのままの形で電子的に記述したものをドキュメント 11 の保護に適用した場合について説明する。また、ユーザ端末 4 には、表示装置 (例えば、LCD)、入力装置 (例えば、キーボード)、記録装置 (例えば、FDD、HDD) などを備えたコンピュータ端末を適用できる。なお、ユーザ端末 4 にはドキュメント 11 に対するアクセスを行うためのドキュメントアクセスプログラムが実装されている。また、ユーザ端末 4 には、プリンタが接続されていることとする。

【0106】

ドキュメントアクセスプログラムは、ユーザ端末 4 の使用者 (ユーザ) の入力

操作に応じ、保護ドキュメント 13 を復号化するとともに、設定されている処理要件に応じた処理を自身で行うか、あるいはプリンタなどに実行させる処理を行うプログラムである。

【0107】

ドキュメント保護プログラム 21 は、アクセス制御サーバ 2 の管理者（ドキュメント 11 の配布者）の入力操作に応じた処理要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEA など）を用いてドキュメント 11 を暗号化し、保護ドキュメント 13 を生成する処理を行う。

【0108】

アクセス制御サーバ 2 は、ユーザ端末 4 のユーザがドキュメント 11（保護ドキュメント 13）にアクセスしようとする場合に、自身が記録保持しているセキュリティポリシーを参照し、保護ドキュメント 13 にアクセスする権限があるか否か、処理要件がどのように設定されているかを取得する。アクセス制御サーバ 2 は、セキュリティポリシーのデータをどのような形で記録保持していても構わない。なお、セキュリティポリシーのデータは、XML を用いて記述されているもよい。

【0109】

アクセス制御サーバ 2 は、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベースと、各保護ドキュメント 13 にどのようなセキュリティ属性が設定されているかを示す情報及びその保護ドキュメント 13 を復号化する為の暗証鍵が関連づけられて登録されるセキュリティ属性データベースと、セキュリティポリシー（例えば図 10）と、ファイルタイプとセキュリティ属性の対応を示すマッピングテーブル（例えば図 11）と、を有する。

【0110】

ユーザデータベースは、ユーザごとにカテゴリと階級とを別々の属性として管理する。例えば、Windows（登録商標）Domain のユーザ管理機構を利用してユーザを管理するような場合には、グループアカウントとして Technical_Medium のようなものを生成し、Ichiro というユーザをそのグループに所属させるようにしてもよい。所属グループの命名規則をこの

ように設定しておくことで、カテゴリと階級とを管理することが可能となる。

【0111】

以下、セキュリティポリシーを用いて、ドキュメント 11 にセキュリティ処理を施す場合の文書発行ワークフローシステムの動作を説明する。

【0112】

ワークフロープログラム 20 は、ワークフロー情報 12 a 生成後、ファイルタイプとセキュリティ属性とが関連付けられているマッピングテーブルを参照して、ワークフロー情報 12 a で指定されたファイルタイプに対応したセキュリティ属性と、ドキュメント 11 とをドキュメント保護プログラム 21 に渡す。例えば、ワークフロー情報 12 a で RESEARCH_PLAN が指定された場合には、ワークフロープログラム 20 は、ドキュメント 11 およびそのドキュメント ID とともに、図 11 のテーブルに基づいたセキュリティ属性として「Technical」と「Medium」をドキュメント保護プログラム 21 に渡す。

【0113】

セキュリティ属性を取得したドキュメント保護プログラム 21 は、復号に使用する暗号鍵を生成し、生成した暗号鍵とセキュリティ属性とをドキュメント ID に関連づけて記録装置 22 に登録する。

また、ドキュメント保護プログラム 21 は、暗号鍵を用いて暗号化したドキュメント 11 に対してドキュメント ID を付加して保護ドキュメント 13 を生成する。

【0114】

アクセス制御サーバ 2 は、ドキュメント保護プログラム 21 が生成した保護ドキュメント 13 を例えばネットワークを介して送信するなどしてユーザ端末 4 に受け渡す。

【0115】

ユーザが、ユーザ端末 4 に対して保護ドキュメント 13 へのアクセスを指示すると、アクセス要求されたユーザ端末 4 は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメントアクセスプログラムは、ユーザ端末 4 の表示装置にメッセージを表示するなどして、ユ

ーザ名とパスワードの入力を要求する。

【0 1 1 6】

ドキュメントアクセスプログラムは、ユーザから入力されたユーザ名とパスワードとをアクセス制御サーバ2へ送信して、ユーザ認証を要求する。

【0 1 1 7】

アクセス制御サーバ2は、ユーザ端末4から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【0 1 1 8】

ユーザを特定すると、アクセス制御サーバ2は、セキュリティ属性データベースを参照し、保護ドキュメント13に設定されているセキュリティ属性の種類を特定する。

アクセス制御サーバ2は、ユーザDBから取得したユーザの階級を示す情報及び、ドキュメント11に設定されているセキュリティ属性とに基づいて、ドキュメント11に対するアクセス権限がユーザにあるか否かや、ユーザがドキュメント11にアクセスする際にはどのような処理要件が設定されているのかを取得する。

【0 1 1 9】

ユーザにドキュメント11にアクセスする権限がある場合、アクセス制御サーバ2は、アクセスが許可されていることを示す許可情報とともに、保護ドキュメント13を復号化するための暗号鍵とユーザがドキュメント11にアクセスする際の処理要件とをユーザ端末4へ送信し、ドキュメントアクセスプログラムに受け渡す。

【0 1 2 0】

アクセス制御サーバ2から許可情報とともに、暗証鍵と処理要件とを取得したドキュメントアクセスプログラムは、暗号鍵を用いて保護ドキュメント13を復号化してドキュメント11に復元する。

例えば、ドキュメントアクセスプログラムは、ドキュメント11の印刷を行う場合、処理要件を満たすように自身に接続されているプリンタに印刷処理を実行させる。例えば、ドキュメント11にBDPが印刷の処理要件として設定されて

いる場合には、ドキュメント 1 1 の内容とともに地紋画像を印刷する。

【0 1 2 1】

これにより、ドキュメント 1 1 を印刷する際に、予め設定されたセキュリティ属性に応じた処理要件を強制することが可能となる。

【0 1 2 2】

なお、本発明の第 1 および第 2 の実施形態では、ワークフロープログラム 2 0 とドキュメント保護プログラム 2 1 とは、アクセス制御サーバ 2 に格納され、アクセス制御サーバ 2 を動作させていたが、それぞれ異なった情報処理装置に格納され、それぞれの情報処理装置を動作させるようにしてもよい。

【0 1 2 3】

以上説明したように、本実施形態では、アクセス制御サーバ 2 は、ファイルタイプとセキュリティ属性とを関連付けたテーブルを格納する。従って、ドキュメント 1 1 に係るユーザ I D およびファイルタイプなどの簡単な情報を入力するだけで、セキュリティポリシーに基づいた複数のユーザに対するドキュメント 1 1 へのアクセス制御を容易に行うことが可能となる。

【0 1 2 4】

また、作成クライアントプログラム 1 0 は、ドキュメント 1 1 およびワークフロー情報 1 2 を作成する処理と、ワークフロー情報 1 2 作成画面をディスプレイに表示させる処理と、ドキュメント 1 1 およびワークフロー情報 1 2 を送信させる処理と、を作成者端末 1 のコンピュータに実行させる。

【0 1 2 5】

また、ワークフロープログラム 2 0 は、ワークフロー情報 1 2 a を生成する処理と、承認者端末 3 にドキュメント 1 1 の審査を依頼する旨の情報を送信させる処理と、承認者端末 3 からの「承認」または「却下」を示す情報に基づいてワークフロー情報 1 2 a を書き換える処理と、ACL テンプレートを格納する処理と、承認されたドキュメントの種別の ACL テンプレートを抽出する処理と、抽出した ACL テンプレートに各ユーザ（作成者、承認者、および配布先）に係る情報を挿入してドキュメント 1 1 のアクセス権限を示す ACL を生成する処理と、暗号鍵を生成する処理と、ドキュメント 1 1 のセキュリティ属性を抽出する処理

と、ドキュメント 11 のデータフォーマットを変換する処理と、保護ドキュメント 13 を送信させる処理と、をアクセス制御サーバ 2 に実行させる。

【0126】

また、ドキュメント保護プログラム 21 は、ドキュメント 11 および対応する ACL（またはセキュリティポリシー）に基づいて、プロテクトされたドキュメントである保護ドキュメント 13 を生成する処理と、をアクセス制御サーバ 2 のコンピュータに実行させる。

【0127】

また、承認者クライアントプログラム 30 は、情報の送受信を制御する処理と、情報の表示を制御する処理と、ドキュメントが「承認」または「却下」された旨の情報入力を認識する処理と、「承認」または「却下」された旨の情報の送信を制御する処理と、を承認者端末 3 のコンピュータに実行させる。

【0128】

また、ドキュメントアクセスプログラムは、情報の送受信を制御する処理と、保護ドキュメント 13 を復元する処理と、プリンタに印刷を指示する処理と、をユーザ端末 4 に実行させる。

【0129】

上記の作成者クライアントプログラム 10、ワークフロープログラム 20、ドキュメント保護プログラム 21、承認者クライアントプログラム 30、およびドキュメントアクセスプログラムは、光記録媒体、磁気記録媒体、光磁気記録媒体、または半導体等の記録媒体に記録され、上記の記録媒体からロードされるようにしてもよいし、所定のネットワークを介して接続されている外部機器からロードされるようにしてもよい。

【0130】

なお、上記の実施形態は本発明の好適な実施の一例であり、本発明の実施形態は、これに限定されるものではなく、本発明の要旨を逸脱しない範囲において種々変形して実施することが可能となる。

【0131】

【発明の効果】

以上説明したように、本発明によれば、電子データに係るユーザ I D、およびデータ種別などが示されているワークフロー情報と、アクセス権限情報のテンプレートと、を用いてアクセス権限情報を生成する。従って、電子データに係るユーザ I D およびデータ種別などの簡単な情報を入力するだけで、電子データに対する複数のユーザのアクセス権限情報を容易に生成することが可能となる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態における文書発行ワークフローシステムを示す第 1 の図である。

【図 2】

本発明の第 1 の実施形態における作成者端末のワークフロー情報作成時の画面表示を示す図である。

【図 3】

本発明の第 1 の実施形態におけるワークフロー情報の一例を示す図である。

【図 4】

本発明の第 1 の実施形態における I D が付与されたワークフロー情報を示す図である。

【図 5】

本発明の第 1 の実施形態における文書発行ワークフローシステムを示す第 2 の図である。

【図 6】

本発明の第 1 の実施形態における A C L テンプレートを示す図である。

【図 7】

本発明の第 1 の実施形態における A C L の一例を示す図である。

【図 8】

本発明の第 1 の実施形態におけるユーザ端末による印刷動作を示す図である。

【図 9】

本発明の第 1 の実施形態におけるユーザ端末に設けられている表示装置の画面上に表示されるプリントダイアログを示す図である。

【図 1 0】

本発明の第 2 の実施形態におけるアクセス制御サーバの記録装置に登録されるセキュリティポリシーの一例を示す図である。

【図 1 1】

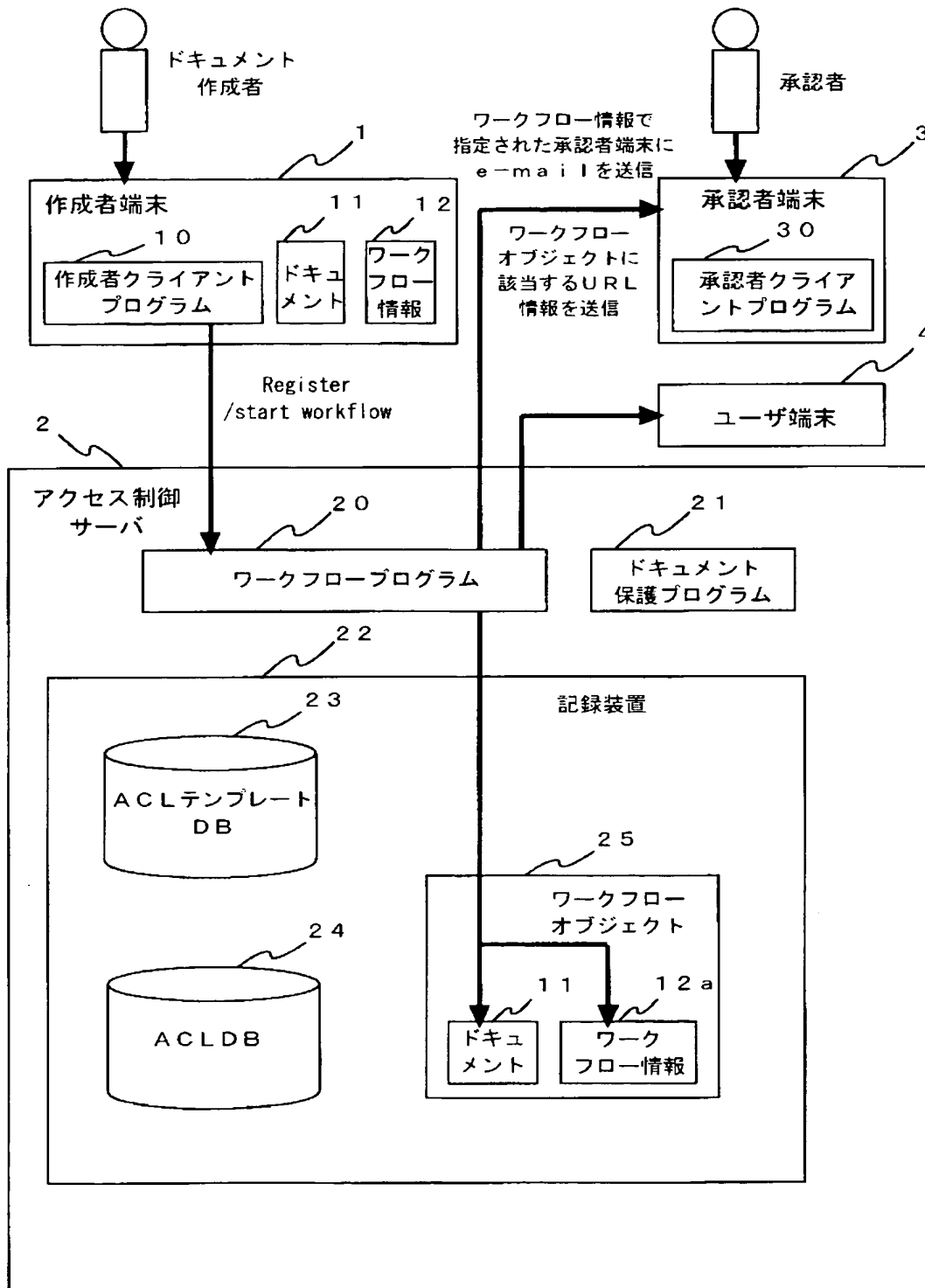
本発明の第 2 の実施形態におけるドキュメントのファイルタイプとセキュリティポリシーとの対応を示すマッピングテーブルを示す図である。

【符号の説明】

- 1 作成者端末
- 2 アクセス制御サーバ
- 3 承認者端末
- 4、4 0 2 ユーザ端末
- 1 0 作成者クライアントプログラム
- 1 1 ドキュメント
- 1 2、1 2 a ワークフロー情報
- 1 3 保護ドキュメント
- 2 0 ワークフロープログラム
- 2 1 ドキュメント保護プログラム
- 2 2 記録装置
- 2 3 A C L テンプレート D B
- 2 4 A C L D B
- 3 0 承認者クライアントプログラム
- 4 0 3 プリンタ
- 4 2 1 ドキュメント印刷プログラム

【書類名】 図面

【図 1】



【図 2】

| ファイル作成画面 | |
|---|---|
| ファイルタイトル： | Development of a new security sysstem |
| ファイルタイプ： | <input type="button" value="▼"/> RESEARCH_PLAN |
| 作成者： | author_00@office.com |
| ファイル内容： | <div>file theme_explanation.doc</div> |
| 配布先： | user_10@office.com, user_11@office.com, user_20@office.com, user_21@office.com |
| 承認者： | approver_01@office.com |
| <input type="button" value="承認（審査）依頼"/> | |

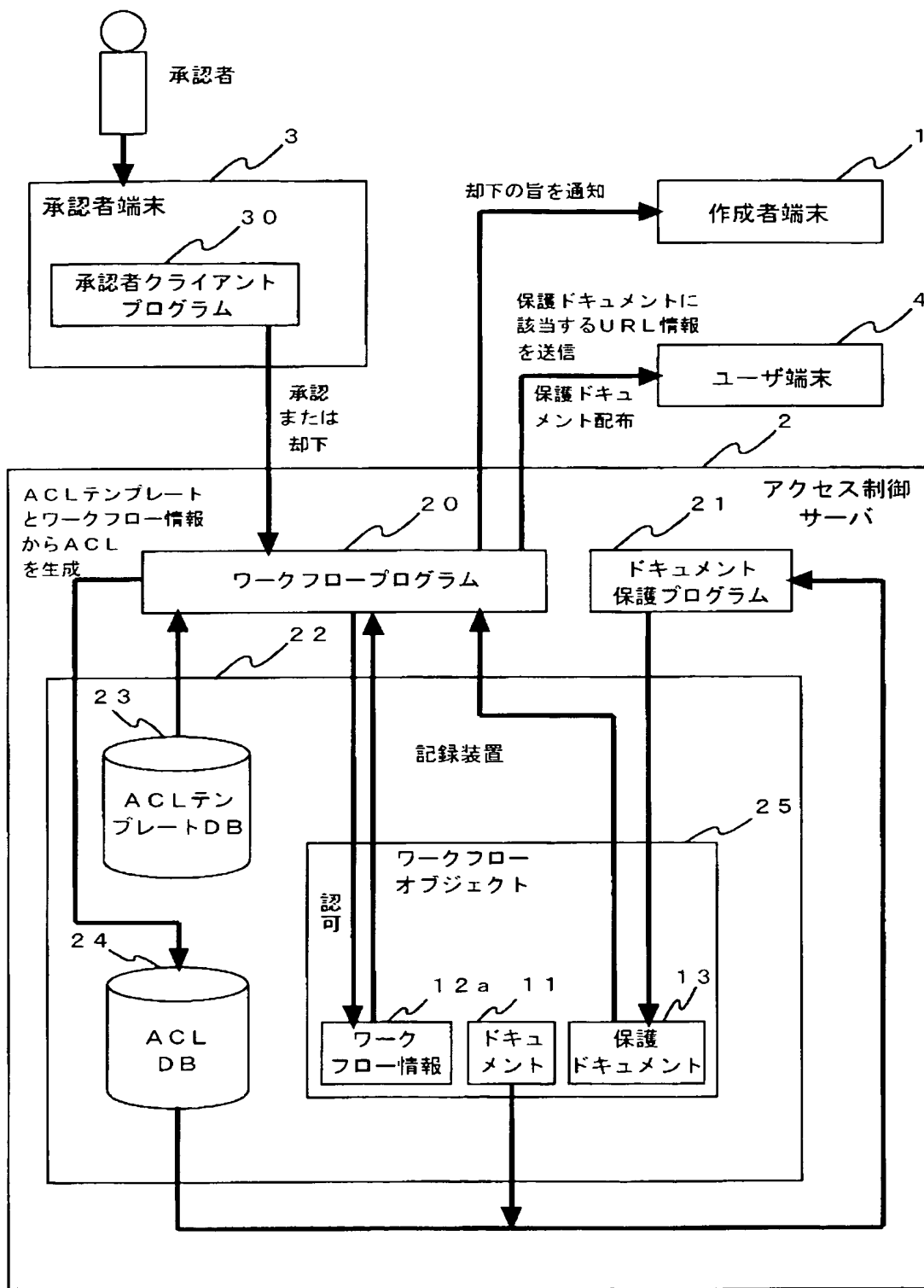
【図 3】

| | |
|---------|--|
| ファイル名 | Development of a new security system |
| ファイルタイプ | RESEACH_PLAN |
| 作成者 | author_00@office.com |
| 承認者 | approver_01@office.com |
| ファイル内容 | theme_explanation.doc |
| 配布先 | user_10@office.com user_11@office.com user_20@office.com user_21@office.com |

【図 4】

```
<?xml version="1.0" encoding="UTF-8"?>
<workflow_info>
  <id>011237835</id>
  <title>Development of a new security sysytem</title>
  <doc_type>RESEARCH_PLAN</doc_type>
  <status>wait_for_approval</status>
  <author>autor_00@office.com</author>
  <approver>approver_01@office.com</approver>
  <distribute_to>user_10@office.com</distribute_to>
  <distributed_to>user_10@office.com</distributed_to>
  <distributed_to>user_10@office.com</distributed_to>
  <distributed_to>user_10@office.com</distributed_to>
</workflow_info>
```

【図 5】



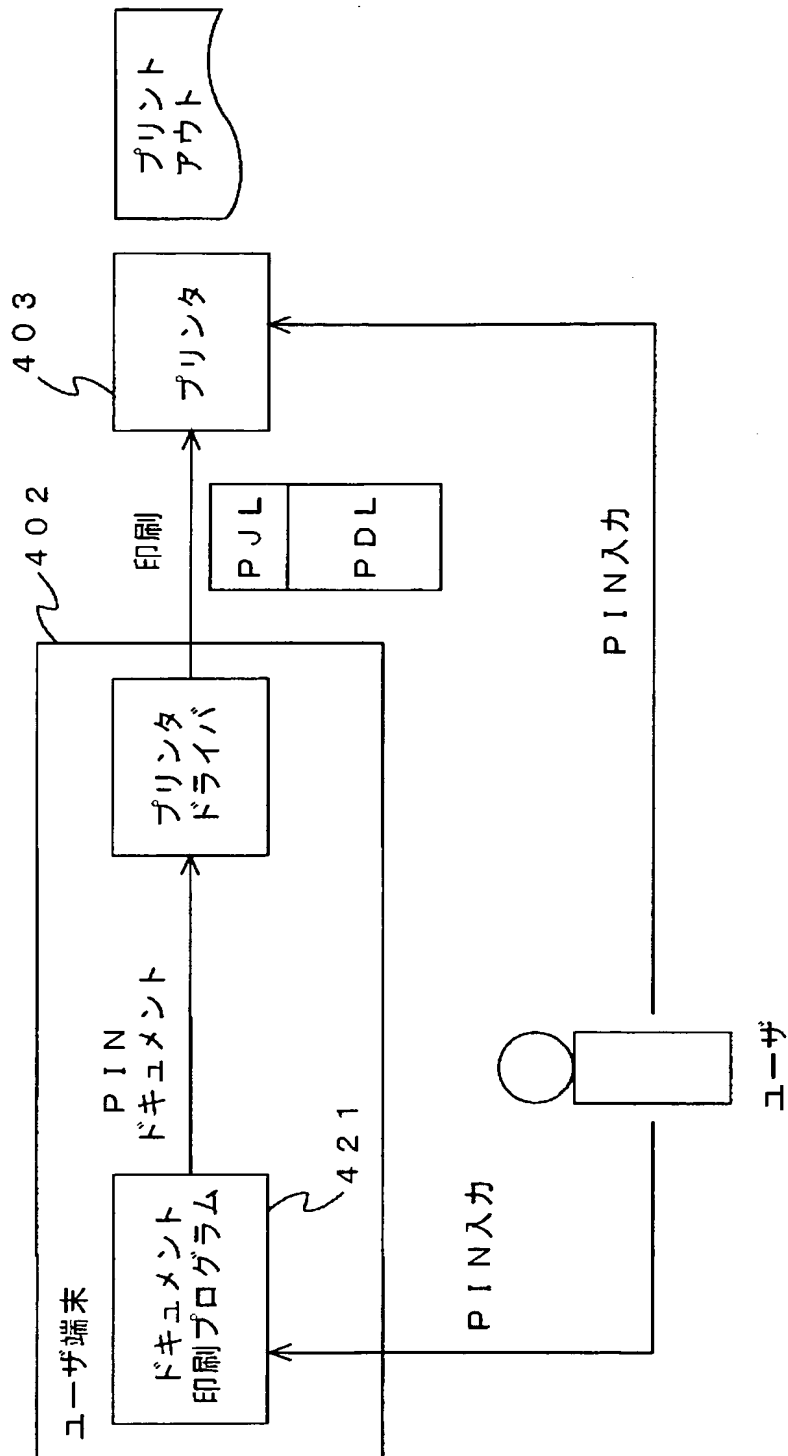
【図 6】

| User type | Access type | Permission | Requirements |
|---------------|-------------|------------|-----------------------------|
| author | Read | Allowed | — |
| | Write | Denied | — |
| | Print | Allowed | PAC(Private Access) |
| | Hardcopy | Allowed | — |
| approver | Read | Allowed | — |
| | Write | Denied | — |
| | Print | Allowed | PAC(Private Access) |
| | Hardcopy | Allowed | — |
| distribute_to | Read | Allowed | — |
| | Write | Denied | — |
| | Print | Allowed | PAC(Private Access) |
| | | | BDP(Background Dot Pattern) |
| | | | EBC(Embedding Barcord) |
| | Hardcopy | Allowed | RAD(Record Audit Data) |

【図 7】

| User type | Access type | Permission | Requirements |
|------------------------|-------------|------------|--|
| author_00@office.com | Read | Allowed | - |
| | Write | Denied | - |
| | Print | Allowed | PAC(Private Access) |
| | Hardcopy | Allowed | - |
| approver_01@office.com | Read | Allowed | - |
| | Write | Denied | - |
| | Print | Allowed | PAC(Private Access) |
| | Hardcopy | Allowed | - |
| user_10@office.com | Read | Allowed | - |
| | Write | Denied | - |
| | Print | Allowed | PAC(Private Access) BDP(Background Dot Pattern) EBC(Embedding Barcord) |
| | Hardcopy | Allowed | RAD(Record Audit Data) |
| user_11@office.com | Read | Allowed | - |
| | Write | Denied | - |
| | Print | Allowed | PAC(Private Access) BDP(Background Dot Pattern) EBC(Embedding Barcord) |
| | Hardcopy | Allowed | RAD(Record Audit Data) |
| user_20@office.com | Read | Allowed | - |
| | Write | Denied | - |
| | Print | Allowed | PAC(Private Access) BDP(Background Dot Pattern) EBC(Embedding Barcord) |
| | Hardcopy | Allowed | RAD(Record Audit Data) |
| user_21@office.com | Read | Allowed | - |
| | Write | Denied | - |
| | Print | Allowed | PAC(Private Access) BDP(Background Dot Pattern) EBC(Embedding Barcord) |
| | Hardcopy | Allowed | RAD(Record Audit Data) |

【図 8】



【図 9】

プリンタ

プリンタ名

プロパティ

状態：通常使うプリンタ：オンライン

種類：●●●●●●●●

印刷範囲

☒ 全ページ

☐ 現在のページ

☐ ページ範囲

開始

終了

印刷部数

プリントダイアログ

この文書は機密文書ですので機密印刷を行います。
暗証番号をセットしてください。
セットした暗証番号をプリンタのところで入力すると
印刷出力されます。

暗証番号

OK

キャンセル

PIN入力ダイアログ

【図 10】

| Document Type | | User Type | | Access Type | Permission | Requirement |
|----------------|-------------|----------------|----------------|-------------|------------|--------------------------|
| Category | Sensitivity | Category | Level | | | |
| Technical | Medium | Technical | Medium High | Read | Allowed | RAD |
| | | | | Print | Allowed | PAC BDP EBC RAD |
| | | | | Hardcopy | Denied | |
| | | | | ... | | |
| Technical | High | Technical | High | ... | | |
| | | | | ... | | |
| | | | | ... | | |
| Human Resource | High | Human Resource | High | Read | Allowed | RAD |
| | | | | Print | Denied | |
| | | | | Hardcopy | Denied | |

【図 1 1】

| Document type | Security attributes | |
|------------------|---------------------|-------------|
| | Category | Sensitivity |
| RESEARCH_PLAN | Technical | Medium |
| GENERAL_CONTRACT | Contract | Basic |
| TOP_SECRET | General | High |



【書類名】 要約書

【要約】

【課題】 電子データに対する利用権限を示すデータ（アクセス）を容易に生成し、その生成した利用権限を示すデータに基づいて電子データに対するアクセス制御を行うアクセス制御サーバ、電子データ発行ワークフロー処理方法、そのプログラム、コンピュータ装置、および記録媒体を提供する。

【解決手段】 アクセス制御サーバ2は、作成者端末1から受信したワークフロー情報12にドキュメントIDを付加してワークフロー情報12aを生成する。アクセス制御サーバ2は、ワークフロー情報12aのファイルタイプに対応したACLテンプレートを抽出する。アクセス制御サーバ2は、抽出したACLテンプレートにワークフロー情報12aの作成者、承認者、ドキュメント配布先のユーザのユーザIDを挿入してACLを生成し、生成したACLに基づいてドキュメント11に対するアクセス制御を行う。

【選択図】 図1



特願 2 0 0 2 - 2 9 9 6 5 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日 1 9 9 0 年 8 月 2 4 日
 [変更理由] 新規登録
 住 所 東京都大田区中馬込 1 丁目 3 番 6 号
 氏 名 株式会社リコー

2. 変更年月日 2 0 0 2 年 5 月 1 7 日
 [変更理由] 住所変更
 住 所 東京都大田区中馬込 1 丁目 3 番 6 号
 氏 名 株式会社リコー